

# Recurrence Sequences

Graham Everest

Alf van der Poorten

Igor Shparlinski

Thomas Ward

SCHOOL OF MATHEMATICS, UNIVERSITY OF EAST ANGLIA, NORWICH, ENGLAND

CENTRE FOR NUMBER THEORY RESEARCH, MACQUARIE UNIVERSITY, SYDNEY, AUSTRALIA

CENTRE FOR NUMBER THEORY RESEARCH, MACQUARIE UNIVERSITY, SYDNEY, AUSTRALIA

SCHOOL OF MATHEMATICS, UNIVERSITY OF EAST ANGLIA, NORWICH, ENGLAND

2000 *Mathematics Subject Classification.* 11B37, 11T23, 11B39, 11G05, 33B10,  
11J71, 11K45, 11B85, 37B15, 94A60

# Contents

Notation	vii
Introduction	ix
Chapter 1. Definitions and Techniques	1
1.1. Main Definitions and Principal Properties	1
1.2. $p$ -adic Analysis	12
1.3. Linear Forms in Logarithms	15
1.4. Diophantine Approximation and Roth's Theorem	17
1.5. Sums of $S$ -Units	19
Chapter 2. Zeros, Multiplicity and Growth	25
2.1. The Skolem–Mahler–Lech Theorem	25
2.2. Multiplicity of a Linear Recurrence Sequence	26
2.3. Finding the Zeros of Linear Recurrence Sequences	31
2.4. Growth of Linear Recurrence Sequences	31
2.5. Further Equations in Linear Recurrence Sequences	37
Chapter 3. Periodicity	45
3.1. Periodic Structure	45
3.2. Restricted Periods and Artin's Conjecture	49
3.3. Problems Related to Artin's Conjecture	52
3.4. The Collatz Sequence	61
Chapter 4. Operations on Power Series and Linear Recurrence Sequences	65
4.1. Hadamard Operations and their Inverses	65
4.2. Shrinking Recurrence Sequences	71
4.3. Transcendence Theory and Recurrence Sequences	72
Chapter 5. Character Sums and Solutions of Congruences	75
5.1. Bounds for Character Sums	75
5.2. Bounds for other Character Sums	83
5.3. Character Sums in Characteristic Zero	85
5.4. Bounds for the Number of Solutions of Congruences	86
Chapter 6. Arithmetic Structure of Recurrence Sequences	93
6.1. Prime Values of Linear Recurrence Sequences	93
6.2. Prime Divisors of Recurrence Sequences	95
6.3. Primitive Divisors and the Index of Entry	103
6.4. Arithmetic Functions on Linear Recurrence Sequences	109
6.5. Powers in Recurrence Sequences	113

Chapter 7. Distribution in Finite Fields and Residue Rings	117
7.1. Distribution in Finite Fields	117
7.2. Distribution in Residue Rings	119
Chapter 8. Distribution Modulo 1 and Matrix Exponential Functions	127
8.1. Main Definitions and Metric Results	127
8.2. Explicit Constructions	130
8.3. Other Problems	134
Chapter 9. Applications to Other Sequences	139
9.1. Algebraic and Exponential Polynomials	139
9.2. Linear Recurrence Sequences and Continued Fractions	145
9.3. Combinatorial Sequences	150
9.4. Solutions of Diophantine Equations	157
Chapter 10. Elliptic Divisibility Sequences	163
10.1. Elliptic Divisibility Sequences	163
10.2. Periodicity	164
10.3. Elliptic Curves	165
10.4. Growth Rates	167
10.5. Primes in Elliptic Divisibility Sequences	169
10.6. Open Problems	174
Chapter 11. Sequences Arising in Graph Theory and Dynamics	177
11.1. Perfect Matchings and Recurrence Sequences	177
11.2. Sequences arising in Dynamical Systems	179
Chapter 12. Finite Fields and Algebraic Number Fields	191
12.1. Bases and other Special Elements of Fields	191
12.2. Euclidean Algebraic Number Fields	196
12.3. Cyclotomic Fields and Gaussian Periods	202
12.4. Questions of Kodama and Robinson	205
Chapter 13. Pseudo-Random Number Generators	211
13.1. Uniformly Distributed Pseudo-Random Numbers	211
13.2. Pseudo-Random Number Generators in Cryptography	220
Chapter 14. Computer Science and Coding Theory	231
14.1. Finite Automata and Power Series	231
14.2. Algorithms and Cryptography	241
14.3. Coding Theory	247
Sequences from the on-line Encyclopedia	255
Bibliography	257
Index	309

## Notation

Particular notation used is collected at the start of the index; some general notation is described here.

- $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}_+$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  denote the natural numbers, integers, non-negative integers, rational numbers, real numbers, and complex numbers, respectively;
- $\mathbb{Q}_p$ ,  $\mathbb{Z}_p$ ,  $\mathbb{C}_p$  denote the  $p$ -adic rationals, the  $p$ -adic integers, and the completion of the algebraic closure of  $\mathbb{Q}_p$ , respectively;
- $\text{ord}_p z$  is the  $p$ -adic order of  $z \in \mathbb{C}_p$ ;
- $\mathbb{P}$  is the set of prime numbers;
- $\mathcal{R}$  is a commutative ring with 1;
- $\mathbb{F}_q$  is a field with  $q = p^r$  elements,  $p \in \mathbb{P}$ ,  $r \in \mathbb{N}$ , and  $\mathbb{F}_q^*$  is its multiplicative group;
- $\mathbb{F}_p$ ,  $p \in \mathbb{P}$  is identified with the set  $\{0, 1, \dots, p-1\}$ ;
- given a field  $\mathbb{F}$ ,  $\overline{\mathbb{F}}$  denotes the algebraic closure of  $\mathbb{F}$ ; thus  $\overline{\mathbb{Q}}$  is the field of all algebraic numbers;
- for any ring  $\mathcal{R}$ ,  $\mathcal{R}[X]$ ,  $\mathcal{R}(X)$ ,  $\mathcal{R}[[X]]$ ,  $\mathcal{R}((X))$  denote the ring of polynomials, the field of rational functions, the ring of formal power series, and the field of formal Laurent series over  $\mathcal{R}$ , respectively;
- $\mathbb{Z}_{\mathbb{K}}$  denotes the ring of integers of the algebraic number field  $\mathbb{K}$ ;
- $H(f)$  denotes the naïve height of  $f \in \mathbb{Z}[x_1, \dots, x_m]$ , that is, the greatest absolute value of its coefficients;
- $\text{gcd}(a_1, \dots, a_k)$  and  $\text{lcm}(a_1, \dots, a_k)$  respectively denote the greatest common divisor and the least common multiple of  $a_1, \dots, a_k$  (which may be integers, ideals, polynomials, and so forth);
- $\varepsilon$  denotes any fixed positive number (for example, the implied constants in the symbol  $O$  may depend on  $\varepsilon$ );
- $\delta_{ij}$  denotes Kronecker's  $\delta$ -function:  $\delta_{ij} = 1$  if  $i = j$ , and  $\delta_{ij} = 0$  otherwise;
- $\mu(k)$ ,  $\varphi(k)$ ,  $\tau(k)$ ,  $\sigma(k)$  respectively denote the Möbius function, the Euler function, the number of integer positive divisors of  $k$ , and the sum of the integer positive divisors of  $k$ , where  $k$  is some non-zero integer;
- $\nu(k)$ ,  $P(k)$ ,  $Q(k)$  respectively are the number of distinct prime divisors of  $k$ , the greatest prime divisor of  $k$ , and the product of the prime divisors of  $k$ ; thus, for example:  $\nu(12) = 2$ ,  $P(12) = 3$ , and  $Q(12) = 6$ ;
- for a rational  $r = k/\ell$  with  $\text{gcd}(k, \ell) = 1$ ,  $P(r) = \max\{P(k), P(\ell)\}$  and  $Q(r) = \max\{Q(k), Q(\ell)\}$ ;
- $\pi(x)$  is the number of prime numbers not exceeding  $x$ ;
- $|X|$  denotes the cardinality of the set  $X$ ;
- $\log x = \log_2 x$ ,  $\ln x = \log_e x$ ;
- $\text{Log } x = \log x$  if  $x > 2$ , and  $\text{Log } x = 1$  otherwise;

- a constant is *effective* if it can be computed in a finite number of steps from starting data;
- $C(\lambda_1, \lambda_2, \dots)$  or  $c(\lambda_1, \lambda_2, \dots)$  denotes a constant depending on the parameters  $\lambda_1, \lambda_2, \dots$ . Such constants may be supposed to be effective, unless it is pointed out explicitly that they are not;
- a statement  $S(x)$  is true for almost all  $x \in \mathbb{N}$  if the statement holds for  $N + o(N)$  values of  $x \leq N$ ,  $N \rightarrow \infty$ . Similarly, a statement  $S(p)$  is true for almost all  $p \in \mathbb{P}$  if it holds for  $\pi(N) + o(\pi(N))$  values of  $p \leq N$ ,  $N \rightarrow \infty$ ;
- the symbol  $\square$  denotes the end of a proof.

## Introduction

The importance of recurrence sequences hardly needs to be explained. Their study is plainly of intrinsic interest and has been a central part of number theory for many years. Moreover, these sequences appear almost everywhere in mathematics and computer science. For example, the theory of power series representing rational functions [1026], pseudo-random number generators ([935], [936], [938], [1277]),  $k$ -regular [76] and automatic sequences [736], and cellular automata [780]. Sequences of solutions of classes of interesting Diophantine equations form linear recurrence sequences — see [1175], [1181], [1285], [1286]. A great variety of power series, for example zeta-functions of algebraic varieties over finite fields [725], dynamical zeta functions of many dynamical systems [135], [537], [776], generating functions coming from group theory [1110], [1111], Hilbert series in commutative algebra [788], Poincaré series [131], [287], [1110] and the like — are all known to be rational in many interesting cases. The coefficients of the series representing such functions are linear recurrence sequences, so many powerful results from the present study may be applied. Linear recurrence sequences even participated in the proof of Hilbert’s Tenth Problem over  $\mathbb{Z}$  ([786], [1319], [1320]). In the proceedings [289], the problem is resolved for many other rings. The article [998] by Pheidias suggests using the arithmetic of bilinear recurrence sequences to settle the still open rational case.

Recurrence sequences also appear in many parts of the mathematical sciences in the wide sense (which includes applied mathematics and applied computer science). For example, many systems of orthogonal polynomials, including the Tchebychev polynomials and their finite field analogues, the Dickson polynomials, satisfy recurrence relations. Linear recurrence sequences are also of importance in approximation theory and cryptography and they have arisen in computer graphics [799] and time series analysis [136].

We survey a selection of number-theoretic properties of linear recurrence sequences together with their direct generalizations. These include non-linear recurrence sequences and exponential polynomials. Applications are described to motivate the material and to show how some of the problems arise. In many sections we concentrate on particular properties of linear recurrence sequences which are important for a variety of applications. Where we are able, we try to consider properties that are particularly instructive in suggesting directions for future study.

Several surveys of properties of linear recurrence sequences have been given recently; see, for example, [215], [725, Chap. 8], [822], [827], [899], [914], [1026], [1181], [1202], [1248], [1285], [1286]. However, they do not cover as wide a range of important features and applications as we attempt here. We have relied on these surveys a great deal, and with them in mind, try to use the ‘covering radius 1’ principle: For every result not proved here, either a direct reference or a pointer to

an easily available survey in which it can be found is given. For all results, we try to recall the original version, some essential intermediate improvements, and — up to the authors' limited knowledge — the best current form of the result.

Details of the scope of this book are clear from the table of contents. In Chapters 1 to 8, general results concerning linear recurrence sequences are presented. The topics include various estimates for the number of solutions of equations, inequalities and congruences involving linear recurrence sequences. Also, there are estimates for exponential sums involving linear recurrence sequences as well as results on the behaviour of arithmetic functions on values of linear recurrence sequences. In Chapters 9 to 14, a selection of applications are given, together with a study of some special sequences. In some cases, applications require only the straightforward use of results from the earlier chapters. In other cases the technique, or even just the spirit, of the results are used. It seems almost magical that, in many applications, linear recurrence sequences show up from several quite unrelated directions. A chapter on elliptic divisibility sequences is included to point out the beginning of an area of development analogous to linear recurrence sequences, but with interesting geometric and Diophantine methods coming to the fore. A chapter is also included to highlight an emerging overlap between combinatorial dynamics and the theory of linear recurrence sequences.

Although objects are considered over different rings, the emphasis is on the conventional case of the integers. A linear recurrence sequence over the integers can often be considered as the trace of an exponential function over an algebraic number field. The coordinates of matrix exponential functions satisfy linear recurrence relations. Such examples suggest that a single exponential only *seems* to be less general than a linear recurrence sequence. Of course that is not quite true, but in many important cases links between linear recurrence sequences and exponential functions in algebraic extensions really do play a crucial role. Michalev and Nechaev [827] give a survey of possible extensions of the theory of linear recurrence sequences to a wide class of rings and modules.

For previously known results, complete proofs are generally not given unless they are very short or illuminating. The underlying ideas and connections with other results are discussed briefly. Filling the gaps in these arguments may be considered a useful (substantial) exercise. Several of the results are new; for these complete proofs are given.

Some number-theoretic and algebraic background is assumed. In the text, we try to motivate the use of deeper results. A brief survey of the background material follows. First, some basic results from the theory of finite fields and from algebraic number theory will be used. These can be found in [725] and [909], respectively. Also standard results on the distribution of prime numbers, in particular the Prime Number Theorem  $\pi(x) \sim x/\ln x$ , will be used. All such results can easily be found in [1049], and in many other textbooks. Much stronger results are known, though these subtleties will not matter here. The following well-known consequences of the Prime Number Theorem,

$$k \geq \varphi(k) \gg k/\text{Log log } k, \quad \nu(k) \ll \text{Log } k/\text{Log log } k$$

and

$$P(k) \gg \nu(k) \text{Log } \nu(k), \quad Q(k) \geq \exp((1 + o(1))\nu(k))$$

will also be needed.

A second tool is  $p$ -adic analysis [29], [131], [620]; in particular Strassmann's Theorem [1261], sometimes called the  $p$ -adic Weierstrass Preparation Theorem. Section 1.2 provides a basic introduction to this beautiful theory. At several points in the text, results about recurrence sequences will be given where the most natural proofs seem to come from  $p$ -adic analysis. We can offer no explanation for this phenomenon. For example, in Section 1.2, we give a simple proof of a special case of the Hadamard quotient problem using  $p$ -adic analysis. The general case has now been resolved and the methods are still basically  $p$ -adic. Similarly, when it is applicable,  $p$ -adic analysis produces very good estimates for the *number* of solutions of equations; compare the estimate of [1123] based on new results on  $S$ -unit equations with that of [1038] obtained by the  $p$ -adic method. On the other hand, a disadvantage of this approach is its apparent non-effectiveness in estimating the *size* of solutions.

The simple observation that any field of zero characteristic over which a linear recurrence sequence is defined may be assumed to be finitely generated over  $\mathbb{Q}$  will be used repeatedly. Indeed, it is enough to consider the field obtained from  $\mathbb{Q}$  by adjoining the initial values and the coefficients of the characteristic polynomial. Then, using specialization arguments [1026] and [1037], we may restrict ourselves to studying sequences over an algebraic extension of  $\mathbb{Q}_p$  or even just over  $\mathbb{Q}_p$ , using a nice idea of Cassels [213]. Cassels shows that given any field  $\mathbb{F}$ , finitely generated over  $\mathbb{Q}$ , and any finite subset  $M \in \mathbb{F}$ , there exist infinitely many rational primes  $p$  such that there is an embedding  $\varphi : \mathbb{F} \rightarrow \mathbb{Q}_p$  with  $\text{ord}_p \varphi(\mu) = 0$  for all  $\mu \in M$ . A critical feature is that the embedding is into  $\mathbb{Q}_p$ , rather than a 'brute force' embedding into an algebraic extension of  $\mathbb{Q}_p$ . The upshot is that for many natural problems over general fields of zero characteristic, one can expect to get results that are not worse than the corresponding one in the algebraic number field case, or even for the case of rational numbers. Moreover, there are a number of examples in the case of function fields where even stronger results can be obtained, see [128], [160], [167], [171], [548], [781], [871] [920], [1002], [1041], [1162], [1308], [1309], [1324], [1373].

Thirdly, many results depend on bounds for linear forms in the logarithms of algebraic numbers. Section 1.3 gives an indication of the connection between the theory of linear recurrence sequences and linear forms in logarithms by considering the apparently simple question: How quickly does a linear recurrence sequence grow? After the first results of Baker [50], [51], [52], [53], [54], [55], and their  $p$ -adic generalizations, for example those of van der Poorten [1017], a vast number of further results, generalizations and improvements have been obtained; appropriate references can be found in [1324]. For our purposes, the modern sharper bounds do not imply any essentially stronger results than those relying on [55] and [1017]. In certain cases more recent results do allow the removal of some logarithmic terms; [1369] is an example. We mostly content ourselves with consequences of the relatively old results.

Fourthly and finally, several results on growth rate estimates or zero multiplicity are based upon properties of sums of  $S$ -units. Specifically, linear recurrence sequences provide a special case of  $S$ -unit sums. Section 1.5 gives a basic account of the way results about sums of  $S$ -units can be applied to linear recurrence sequences. This does not do justice to the full range of applicability of results about sums of  $S$ -units — applications will reverberate throughout the text.

In surveys such as this, it is conventional to attach a list of open questions. Rather than doing this, the best current results known to the authors are presented; if a generalization is straightforward and can be done in the framework of the same arguments that is noted. Other generalizations or improvements should be considered implicit research problems. We do however mention attempts at improvements which seem hopeless in the light of today's knowledge.

Finally, we add several words about what we do not deal with. First, it is striking to note that the binary recurrence  $u(n+2) = u(n+1) + u(n)$ , one of the simplest linear recurrences whose solutions are not geometric progressions, has been a subject of mathematical scrutiny certainly since the publication of Leonardo of Pisa's *Liber abaci* in 1202 [1212]. Indeed, this recurrence has an entire journal devoted to it [113]. This volume is more egalitarian; with a few exceptions, no special properties of individual recurrences will be discussed. Several specific sequences arise as examples; the most important of these are listed with their identifying numbers in Sloane's Online Encyclopedia of Integer Sequences [1222] in an Appendix on page 254.

Second, one could write an enormous book devoted to one particular case of linear recurrence sequences — polynomials. We do not deal with polynomials *per se*; extensive treatments are in [1116] and [1120]. Nonetheless, this case alone justifies the great interest in general linear recurrence sequences. Therefore, we give several applications to polynomials but such applications are obtained using partially hidden — although not too deep — links between polynomials and linear recurrence sequences.

Third, a huge book could be written dealing with exponential polynomials as examples of entire functions and therefore, ultimately, with analytic properties of those functions. We barely consider any analytical features of exponential polynomials, though we mention some relevant results about the distribution of their zeros. We do not deal with analytical properties of iteration of polynomial mappings. Thus the general field of complex dynamics, and the celebrated Mandelbrot set, is outside our scope. (Recall that the Mandelbrot set is the set of points  $c \in \mathbb{C}$  for which the sequence of polynomial iterations  $z(k) = z(k-1)^2 + c$ ,  $z(0) = 0$ , is bounded; for details we refer to [154].) However, in Chapter 3 we do consider some simple periodic properties of this and more general mappings.

Fourth, as we mentioned, general statements about the behaviour — both Archimedean and non-Archimedean — of sums of  $S$ -units lie in the background of important results on linear recurrence sequences. Nonetheless, we do not deal with sums of  $S$ -units or their applications systematically. On the topic generally, we first recommend the pioneering papers [376] and [1037] which appeared independently and contemporaneously (the latter as a preprint [1019] of Macquarie University in 1982). We point particularly to the book [1181] and the excellent survey papers [378], [380], [381], [382], [503], [1128], [1175], [1285], [1286].

On the other hand, we do present some less well-known results about finitely generated groups, such as estimates of the size of their reduction modulo an integer ideal in an algebraic number field, and on the testing of multiplicative independence of their generators. When results on  $S$ -unit sums are applied to linear recurrence sequences, an induction argument usually allows the conditions on non-vanishing proper sub-sums to be eliminated (such conditions are unavoidable in the general study of  $S$ -unit sums).

Despite the large number of references, no systematic attempt has been made to trace the history of major results that have influenced the subject. No single book on the history of this huge topic could hope to be definitive. However — Leonardo of Pisa notwithstanding — it is reasonable to view the modern study of the arithmetic of recurrence sequences as having been given essential impetus by the remarkable work of François Édouard Anatole Lucas (1842–1891); many of the themes developed in this book originate in his papers (see [283] and [1354] for some background on his life and work, and [517] for a full list of his publications and some of his unpublished work).

The bibliography reflects the interests and biases of the authors, and some of the entries are to preliminary works. The authors extend their thanks to the many workers whose contributions have given them so much pleasure and extend their apologies to those whose contributions have not been cited. The authors also thank many people for help with corrections and references, particularly Christian Ballot, Daniel Berend, Keith Briggs, Sheena Brook, Susan Everest, Robert Laxton, Pieter Moree, Patrick Moss, Władysław Narkiewicz, James Propp, Michael Somos, Shaun Stevens, Zhi-Wei Sun and Alan Ward.

*Alf van der Poorten & Igor Shparlinski*  
Centre for Number Theory Research  
Macquarie University  
Sydney  
alf@math.mq.edu.au  
igor@comp.mq.edu.au

*Graham Everest & Thomas Ward*  
School of Mathematics  
University of East Anglia  
Norwich  
g.everest@uea.ac.uk  
t.ward@uea.ac.uk